12 March 1982

MEMORANDUM FOR THE RECORD

SUBJECT: Potential Security Exposure

1. Reports have appeared in the press describing "a newly discovered method of breaking into computer files that may be the most serious security problem ever in the field." The details are not revealed, but the technique is supposed to be simple and can be used to violate the integrity of many timesharing systems.

2. We have a copy of the original report issued by the Stanford Research Institute. The technique that was discovered last year at the University of California at Berkeley had already been encountered by the Agency sometime around 1974. The method is indeed simple:

a. Two kinds of data can be sent to a terminal. There are the conventional characters such as letters, numbers and symbols which convey information to the reader. There are also special characters that are used by the computer to control the terminal. These "control" characters are not displayed upon the screen, but instead cause the terminal to do something special. It is common for control characters to be intermixed with ordinary data. I or example, a "control-G" operation causes the bell on most terminals to ring; a "control-J" causes the cursor to jump down one line. There is nothing particularly radical about this concept; it is simply how many computers work.

b. Timesharing computers allow anywhere from a handful to hundreds of people to use a single computer concurrently. Considerable study has been given to the problem of keeping one user's data safe from unauthorized examination or alteration by others. While not absolutely safe, most modern computers offer an adequate level of privacy. Most timesharing systems also allow two people who are using the computer at the same time to send messages to one another. A user employs a system command to send a message to a fellow user. The computer will normally wait until a convenient moment to display the message on the receiver's terminal. This occurs when the receiver has finished entering a line of data and hits the "ENTER" or "RETURN" key to indicate that the line is complete. When the message is displayed, it is normally preceded by header information provided by the system identifying the originator of the message. For example:

Smith enters:
message jones time for lunch

Jones sees:
MESSAGE FROM SMITH: TIME FOR LUNCH

SUBJECT: Potential Security Exposure

The ability to send messages is so popular that few constraints are placed upon its use.

c. The security problem arises when a user sends a message to another user that contains control characters. With older terminals, an ill-mannered user could harass another user by sending a message which included a "clear screen" control character. The recipient would see the screen go blank inexplicably, although most systems would display the identity of the originating user for an instant before the screen cleared. The victim is normally surprised because the sender chooses the moment that the message will be transmitted. Since the receiver did not have to take any specific action to see the message, the data displayed upon the terminal appears to be random and nuisance messages are frequently assumed to be problems with the computer.

d. Newer terminals are much more sophisticated and have a much wider range of control characters. It is possible on some modern terminals to send a complicated message that results in a portion of the message being treated as data entered by the user sitting at the receiving terminal. Hence, a clever user could send messages to someone else that result in commands being issued as if they had been entered by that other user. This opens all sorts of possibilities for a sinister computer user. The precise method is different for various models of computer terminals and requires a detailed understanding of the technical characteristics of the hardware. College students are notorious for having the time and curiousity needed to develop the techniques to exploit these vulnerabilities.

e. Most timesharing systems also allow the user to send data files to other users. This gives rise to a different twist of the problem. A sinister user can send a file, or a document in an electronic mail system, that contains control characters and commands. When the receiving user displays the file, the commands are executed. This is part of a classic computer security problem known as the "trojan horse." It is the office automation equivalent of the letter bomb.

f. There is a key difference between the message and file problems. A message appears to the user as a random event; the display of a file requires some action by the recipient. If the terminal screen clears immediately after displaying a document from another user, the victim is much more likely to perceive a cause and effect relationship. This is particularly true if the attacker attempts to destroy the evidence by erasing the file. There are also numerous system features, such as audit trails, that further constrain the usefulness of the file method.

SUBJECT: Potential Security Exposure

The technique uncovered by the Berkeley students is potentially a problem for a wide variety of computer systems. A sinister user would be much more likely to embed terminal control commands in an inter-user message rather than employing a "trojan horse" file; the risk of detection is much less.

3. There are a several approaches that can be taken to eliminate or minimize the vulnerability. Users could be prevented from communicating with each other, but that would not be practical for most systems. Since the exposure is greater with "smart" terminals, the hardware could be "lobotomized" to remove exploitable functions. Again, this is not generally practical. The choice of many computer installations has been to block the message attack entirely by deleting terminal control operations from the text of messages. This is accomplished by a fairly simple modification to the vendor's software. The "trojan horse" file approach is more difficult to block using technical means; user awareness coupled with system management too' can reduce the chance of an attack going undetected.

4. The vulnerability of terminals to control information imbedded in user messages is a problem that is as old as the hills. We have blocked the more dangerous aspects of this security exposure on all of our time-sharing systems. IBM Corporation, the vendor of our systems software, is aware of the problem and is investigating various permanent solutions. It is unfortunate that this issue has been dragged into the open; such matters are better dealt with quietly.